OFFICE OF THE INSPECTOR GENERAL
CORPORATION FOR NATIONAL AND
COMMUNITY SERVICE

Review of The Corporation for National and Community Service's Network and Computer Security Plan

OIG Audit Report Number 01-34
December 11, 2000

Prepared by:

KPMG, LLP
2001 M Street, NW
Washington, DC 20036

Under Corporation for National and Community Service
Office of the Inspector General
Purchase Order # 200008020002
General Services Administration Contract # GS-23F-8127H

This report was issued to Corporation management on May 7, 2001. Under the laws and regulations governing audit follow up, the Corporation must make final management decisions on the report's findings and recommendations no later than November 5, 2001, and complete its corrective actions by May 7,2002. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

CORPORATION
FOR NATIONAL
SERVICE

Office of Inspector General
Corporation for National and Community Service

Review of the Corporation for National and Community Service's Network and Computer Security Plan OIG Audit Report Number 01-34

OMB Circular A-130, "Management of Federal Information Resources," requires that Federal agencies implement and maintain adequate security over information, information systems, and major applications. The Corporation's Network and Computer Security Plan includes a description of the Corporation's computer systems, the major applications, and the security and control procedures in place.

CNS OIG engaged KPMG, LLP to review the plan and to assess the effectiveness of the security policies and procedures. Their report concludes that the Corporation has met the requirements of the Circular with two exceptions for which this report includes recommendations for corrective action. CNS OIG reviewed the report, with which we concur, the work papers supporting its conclusions, and the Corporation's response to the report.

In its response, the Corporation agreed with KPMG's recommendation for the first finding which was to include a summary of the Security Plan in the Corporation's Strategic Information Risk Management Plan as required by Circular A-130. However, the Corporation did not agree with the KPMG's second finding – that there is no separate, specific management authorization for the Internet connection to the Corporation LAN. KPMG did not change the report because CNS failed to provide documentation on this matter either during the audit or as part of the response to the report.

Inspector General
1201 New York Avenue, NW
Washington, DC 20525

Review of the
Corporation for National and Community Service's
Network and Computer Security Plan
Table of Contents

RESULTS IN BRIEF 1

PROJECT OBJECTIVES 1

METHODOLOGY 2

SUMMARY OF NOTIFICATION OF FINDINGS 3

NEW INFORMATION SECURITY LEGISLATION 3

APPENDIX A – NOTIFICATION OF FINDINGS A-1

APPENDIX B – LIST OF DOCUMENTS REVIEWED B-1

APPENDIX C – CORPORATION RESPONSES TO THE DRAFT C-1

2001 M Street, N.W.
Washington, D.C. 20036

Telephone 202 467 3000
Fax 202 833 1350

December 11, 2000

Inspector General
Corporation for National and Community Service:

At your request, KPMG, LLP (KPMG) performed a Network Security Review on the Corporation for National Service (the Corporation). The primary purpose of this review was to:

- review the current network security plan and
- to assess the effectiveness of computer security policy and procedures

Results in Brief

At the time of the assessment, the Corporation met the requirements of OMB Circular A-130, *Management of Federal Information Resources*, with two exceptions:

- A summary of the Security Plan was not incorporated in the recent Corporation Information Management Strategic Plan dated October 19, 2000; and

- There was no document that specifically gave management authorization for interconnection of the Corporation LAN to the Internet.

Neither of these findings has a direct operational impact on information security. But it is recommended that both of these findings be corrected, because they are good management practices and are required by OMB Circular A-130.

Project Objectives

The objective of this project was to assess the effectiveness of the network and computer security policies and procedures at the Corporation for National and Community Service (the Corporation) through a review of the Corporation's compliance with OMB Circular A-130, *Management of Federal Information Resources*. A review was conducted of policies and procedures, as documented in the Corporation's Security Plan, and an assessment was performed of their effectiveness.

KPMG LLP KPMG LLP, a U.S. limited liability partnership, is a member of KPMG International, a Swiss association.

Methodology

The project included an assessment of the Network Security Plan using OMB Circular A-130 as guidance. OMB Circular A-130 is applicable to all agencies where "the term 'agency' means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the Federal government, or any independent regulatory agency", OMB Circular A-130, Section 6.

This review was conducted in three phases. Phase I, the assessment phase, was designed to ensure the existence of documentation that supports OMB Circular A-130 criteria. A list of documentation reviewed during this phase is included in Appendix B.

Phase II entailed verification of the accuracy of the statements made in the documentation received in Phase I. This verification was accomplished through reviews of relevant documentation and interviews with Corporation personnel.

Phase III consisted of the development of a formal report of the review's findings. As the project team identified findings, they were discussed with the Corporation and the OIG. These findings are documented in the form of Notices of Findings (NOF) and are issued to the OIG and the Corporation as attachments to this report.

In addition, a Vulnerability and Penetration Assessment was performed on the Corporation's external and internal networks. More specifically, we attempted to simulate a number of security penetration scenarios, which included the following categories of potential system "abusers":

- an "outsider" with no information about the organization's EDP environment
- an "outsider" with limited information about the organization's EDP environment
- an "insider" with limited knowledge about the EDP environment
- an "insider" with standard client application programmer access to the EDP environment resources.

Our procedures were performed in accordance with *Government Auditing Standards* for performance audits as issued by the Comptroller General of the United States.

Summary of Notification of Findings

A total of two Notification of Findings (NOFs) were issued during the course of the project. The table below contains a synopsis of the findings and the recommendations documented in each NOF located in Appendix A.

Finding	Recommendation
A summary of Security Plans is not incorporated in the Corporation's Information Management Strategic Plan dated October 19, 2000 as required by OMB Circular A-130.	Incorporate Information Security Planning into the Corporation's overall Information Resource Management Planning.
There is a formal Corporation policy (#375) for use of the Internet that is signed by the Chief Operating Officer, but there is no document that specifically gives management authorization for interconnection of the Corporation LAN to the Internet as required by OMB Circular A-130.	Perform a risk analysis for interconnection of the Corporation LAN to the Internet, and obtain specific formal management approval and acceptance of the risks of interconnection of the Corporation LAN to the Internet.

New Information Security Legislation

Although, at the time of the assessment the Corporation generally met the criteria of OMB Circular A-130, new information security legislation, the Government Information Security Reform Act (GISRA), has been enacted that sets a much higher documentation standard than had previously existed. The legislation includes requirements that will impose additional types of workload burdens, such as annual evaluations. It is also anticipated that OMB Circular A-130, which formed the basis for this review, will be greatly modified in the near future to meet the GISRA requirements. An early start on meeting the new requirements is highly recommended.

The Fiscal Year 2001 National Defense Authorization Act became Public Law 106-398 on October 30, 2000. Title X, Subtitle G of the Act is Government Information Security Reform Act (GISRA). Even though it is part of the Defense Authorization Act, Subtitle G's provisions affect all agencies of the Federal Government. It is effective as of November 30, 2000, and expires in two years. The legislation recognizes the highly networked nature of the Federal computing environment and the need for Federal Government interoperability. It seeks to establish a comprehensive framework for information security and to make it an integral component of each agency's business operations.

New provisions of the legislation call for each agency to:

- Have an agency-wide information security architecture
- Have an information security plan for the life cycle of each agency system
- Perform an annual self evaluation of information security controls and techniques
- Have an annual audit of the Information Security evaluation by the IG
- Provide an annual report of the results of each evaluation and audit to OMB

Procedural guidance from OMB and National Institute of Standards and Technology (NIST) may not come until early 2001. But, implementation of GISRA must proceed soon, to be followed by a self-evaluation of the implementation, an audit of the evaluation by the IG and a report by the agency head to OMB. All must be accomplished before the legislated deadline of October 30, 2001.

A modified OMB Circular A-130 to implement GISRA will be forthcoming, and will likely incorporate the Security Assessment Framework developed by the CIO Council and NIST. The CIO - NIST Information Technology Security Assessment Framework seems to establish a more stringent requirement for comprehensive documentation than currently exists.

*****

This report is intended solely for the information and use of the Office of the Inspector General, the management of the Corporation for National and Community Service, and the United States Congress and is not intended to be and should not be used by anyone other than these specified parties.

Felipe Alonso
Partner, KPMG, LLP

Notification of Findings Appendix A

Notification of Finding: Missing summary of the Corporation Security Plans.

Condition: The recently issued Information Management Strategic Plan, dated October 2000, does not contain a summary of the Corporation security plans. (See Binder C, WP #3100, Page 2 of 10)

Criteria: OMB Circular A-130 requires that "A summary of the security plans shall be incorporated into the strategic IRM plan."

Cause: Given the overall level of attention that has been paid to information security, this appears to be an oversight, and not necessarily indicative of a low resource allocation priority.

Effect: The intent of the requirement is to ensure that Information Security is considered during the agency's strategic resource planning and prioritization process. Allocation of sufficient resources to ensure an effective information security program may not otherwise occur.

Recommendation: Information security should be routinely incorporated into the Corporation's annual strategic resource allocation and prioritization processes. This fiscal year, it is recommended that the Corporation use the updated security plans being developed in conjunction with re-accreditation of all Corporation systems, to provide the basis for incorporation of information security into the overall Information Management Strategic Plan dated October 2000. This should be more than just a documentation change, and ought to be accomplished in sufficient time to ensure that information security requirements are appropriately considered during the next budget cycle.

Management Response:

This finding was discussed with Corporation Management on December 14, 2000. The Corporation did not express major disagreement but said that it intends to provide its formal response on any issues related to the finding in its comments on the draft report.

Appendix A

Notification of Findings

Notification of Finding: Missing management authorization for the Internet connection to the Corporation LAN.

Condition: There is no separate, specific management authorization for the Internet connection to the Corporation LAN. (See Binder C, WP #3100, Page 5 of 10)

Criteria: OMB Circular A-130 requires that there be written management authorization for interconnection to other systems.

Cause: Corporation Policy Number 375 is signed by the Chief Operating Officer and establishes rules for Internet and e-mail access control and acceptable use. This formal policy statement indirectly indicates that Corporation management approves in general of having the Internet connection, but is not a clear statement that management understands and accepts the risks inherent in the Internet connection. Acceptance of responsibility for taking the business risks associated with interconnection to the Internet should clearly be done by Corporation top management.

Effect: The formal acceptance by management of the risks of any interconnection to other systems is the intent of the OMB Circular A-130 requirement. Connection to the Internet, particularly, has many inherent risks. Without management understanding of the potential for the loss of information assets or for harm to critical business processes, inappropriate levels of business risk may be taken or insufficient resource allocations made to ensure an effective security program.

Recommendation: Although Corporation management has given a tacit approval of connection to the Internet; a risk assessment for the interconnection of the Corporation LAN with the Internet should be done. The risk assessment need not be done from scratch. Valuable insight into the extent and nature of the risks may be gained from the various audits and evaluations of Corporation security that are underway. Once the risk assessment is completed, it should be used in conjunction with the updated LAN security plan as the basis for specific management authorization of the Internet interconnection.

Appendix A

Notification of Findings

Management Response:

This finding was discussed with Corporation Management on December 14, 2000. The Corporation did not express major disagreement but said that it intends to provide its formal response on any issues related to the finding in its comments on the draft report.

List of Documents Reviewed

Appendix B

CNS Policy #375	Internet an E-mail Access and Acceptable Use	August 23, 1999
CNS Policy #376	Network and Computer Security	November 7, 2000
CNS Policy #377	Computer Property Management	February 17, 2000
CNS Policy #378	Structured System Development Life Cycle Methodology	April 27, 2000
CNS Policy #400	Visitor Procedures for Computer Room 6316	August 22, 2000
CNS Policy #401	Procedural Guidelines for Disabled and Locked Out Accounts	October 13, 2000
CNS Policy #402	Approving Authority Signatures	August 24, 2000
CNS Policy #501	Safeguarding Sensitive Information and Documents	September 21, 1999
CNS Plan	Information Management Strategic Plan	October 19, 2000
CNS Plan	Network Computer Security Plan	October 2000
CNS Plan	CNS-LAN Security Plan	July 1997
CNS Plan	CNS-LAN Contingency Plan	July 1997
CNS Plan	CNS Disaster Recovery Plan	undated, 2000
CNS Report	CNS-LAN Security Controls Review Report	July 1997
CNS Report	CNS-LAN Risk Analysis Report	July 1997
CNS Accreditation	Accreditation Package for CNS-LAN	August 15, 1997
CNS Procedure	Corporation Network Account Creation, Modification and Deletion Procedure	undated, 2000
CNS Procedure	Corporation Windows NT Server Standard Configuration	undated, 2000
CNS Procedure	Corporation Standard Client Configuration	undated, 2000
CNS Procedure	Corporation Backup Schedule	undated, 2000
CNS Procedure	Corporation Network Maintenance Schedule	undated, 2000
CNS Procedure	2000 Annual Information Systems Security Awareness Training document	undated, 2000
CNS Procedure	CNS Computer Incident Response Guidelines	undated, 2000
CNS Procedure	Help Desk Frequently Asked Questions (FAQ)	undated, 2000
CNS Document	Segregation of Duties	undated, 2000

Appendix C

CORPORATION
FOR NATIONAL
SERVICE

March 30, 2001

The Honorable Luise Jordan,
Inspector General
Corporation for National and
Community Service

Dear Ms. Jordan:

The Corporation has reviewed the draft report *Review of the Corporation for National and Community Service's Network and Computer Security Plan* (OIG Audit Report 01-34, dated December 11, 2000). The purpose of KPMG's work was to review the Corporation's network security plan and assess the effectiveness of computer security policy and procedures. The procedures performed by KPMG included sophisticated attempts to penetrate the Corporation's systems as both an "outside" hacker and an "insider." We note with satisfaction that KPMG failed to circumvent the Corporation's security policies and procedures and that it was unsuccessful in its attempts to penetrate the Corporation's systems.

The Corporation is also pleased that, while not explicitly stated, KPMG concluded that the Corporation's network security plan and computer security policy and procedures are effective and efficient. The Corporation has taken the security of its computer resources very seriously and will continue to do so. To this end, the Corporation routinely tests and monitors its systems and contracts with independent EDP consultants to review and test its systems. We also rely on the testing and review that was performed by KPMG on behalf of the Office of the Inspector General and discussed in this report.

The report cites two minor instances where KPMG feels that the Corporation could have better documentation. In the first instance, KPMG recommends that a summary of the Corporation's Security Plan be incorporated into the Corporation's Information Management Strategic Plan. While we do not agree that this is necessary given the Corporation's EDP operating environment, the Corporation will include a summary of the Security Plan in the Strategic Plan.

1201 New York Avenue, NW
Washington, DC 20525
Telephone 202-606-5000

Getting Things Done.
Americorps, National Service
Learn and Serve America
National Senior Corps

In the second instance, KPMG recommends that the Corporation perform a risk assessment for the interconnection to the Internet and that management formally document its authorization of the connection. Prior to implementing the interconnection, the Corporation ***did*** assess the risks related to providing access to the Internet. In fact, senior management were involved in and made the decision to allow access.

For several years prior to senior management making this decision, the Office of Information Technology (OIT) maintained two separate networks, one serviced the internal business needs and the other was solely for Internet access. As technology changed, the need for easier access to the resources available on the Internet grew. Once technology and monitoring tools became sophisticated enough to enable acceptable protection from external threats, management included the necessary funding in the OIT budget for firewall technology and systems monitoring tools to allow the interconnection to the Internet. The initial risk assessment process culminated when the Chief Operating Officer signed the Corporation's policy on e-mail access controls and use of the Internet.

Internet access has become an integral part of the Corporation's network and is regularly assessed by both staff and independent EDP consultants for security vulnerabilities. For example, as part of the recent re-accreditation of the Corporation's network, independent EDP consultants performed a risk assessment of the entire network including the connection with the Internet. This accreditation was also reviewed and approved by senior management. Thus, the Corporation believes that to do additional risk assessments, beyond what has been and is regularly done, would be an inefficient use of its resources.

* *

Finally, the Corporation would like to express its appreciation for the work of KPMG's staff and their flexibility to work around the other pressing responsibilities of the Corporation staff.

Sincerely,

David Spevacek
Chief Information Officer

cc: Wendy Zenker
Bill Anderson

1201 New York Avenue, NW
Washington, DC 20525
Telephone 202-606-5000

Getting Things Done.
Americorps, National Service
Learn and Serve America
National Senior Corps